Oracle® Database Firewall

Installation Guide

Release 5.0

E18693-08

September 2011

ORACLE®

Oracle Database Firewall Installation Guide Release 5.0

E18693-08

Primary Author: Patricia Huey

Contributors: Tammy Bednar, Paul Betteridge, K. Karun, Valarie Moore, Steve Moyle, Stuart Sharp, James Spooner, Ching Tai, Peter Wahl, James Wilson

Contents

4 Updating the Oracle Database Firewall Software

5 Removing Oracle Database Firewall

Index

Preface

Welcome to *Oracle Database Firewall Installation Guide*. This section contains:

Audience

This document is intended for users who are responsible for installing Oracle Database Firewall.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Documents

For more information, see the following documents in the Oracle Database Firewall Release 4.3 documentation set:

- *Oracle Database Firewall Release Notes*
- *Oracle Database Firewall Administration Guide*
- *Oracle Database Firewall Security Management Guide*

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Overview of the Oracle Database Firewall Installation

This chapter covers the following topics:

Downloading the Latest Version of This Manual

You can download the latest version of this manual from the Oracle Database Firewall Web site, which is in the Database section of Oracle Technology Network. The URL is as follows:

`http://www.oracle.com/technetwork/indexes/documentation/index.html`

About Installing Oracle Database Firewall

Oracle Database Firewall is a system for securing and monitoring data in SQL databases. It blocks and produces warnings of attempted attacks, logs activity, and provides intelligent tools to assess vulnerabilities.

The components that you will install are as follows:

- **One or more Database Firewalls.** Each Database Firewall performs the following tasks:
  - Handles real-time recording and analysis of SQL transaction requests and responses from one or more Oracle, Microsoft SQL Server, or Sybase Adaptive Server Enterprise (ASE), Sybase SQL Anywhere, and IBM DB2 LUW databases.
  - Categorizes SQL transactions
  - Enforces data policies
  - Enables real-time alerting and event propagation
  - Sends SQL data from the protected databases to the Oracle Database Firewall Server and then deletes it locally

You will install each Database Firewall onto a Linux server, which will use Oracle Linux. This Linux server will be used exclusively for Database Firewall. *Oracle Database Firewall Administration Guide* describes how to manage the standalone Database Firewall.

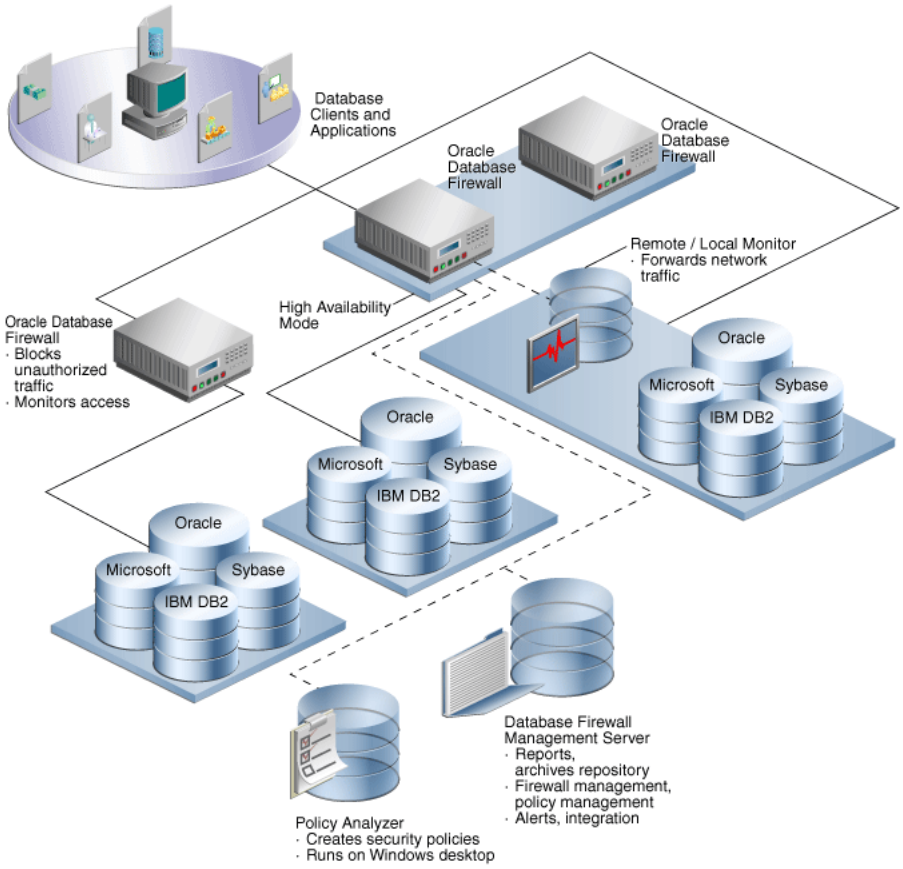
- **One or more Oracle Database Firewall Management Servers.** The Management Server performs the following tasks:
  - Aggregates SQL data from one or more Database Firewalls
  - Serves as a reporting platform for business reports that describe this SQL data
  - Centralizes the distribution of data control policies, but still enables the use of different policies for specific databases
  - Stores and manages log files, including archiving and restoring the log files
  - Remotely manages all Database Firewalls that are connected to it
  - Integrates with third-party applications, such as HP ArcSight SIEM

  You will install each Management Server onto an Intel x86 server, which will use Oracle Linux. This Linux server will be used exclusively for Management Server. *Oracle Database Firewall Administration Guide* describes how to manage the Oracle Database Firewall Management Server.
- **One or more Oracle Database Firewall Analyzers.** The Analyzer reads the logs created by the Database Firewalls to create or update the policy used to block, alert, log, or permit SQL statements for the database. *Oracle Database Firewall Security Management Guide* describes how to use the Analyzer. You will install the Analyzer on a Microsoft Windows client computer.

After you install these components, you must add the databases that you want to monitor, and configure remote or local monitoring for each database. *Oracle Database Firewall Administration Guide* describes how to configure your databases to connect to Oracle Database Firewall. For a list of supported database platforms for these databases, see "Supported Database Versions" on page 2-2.

Figure 1–1 illustrates the architecture of your system after you have installed and configured Oracle Database Firewall. This diagram shows a high availability configuration for two of the Database Firewalls. "Deployment Scenarios" on page 1-4 describes other possible deployments, including high availability configurations.) The diagram also shows remote and local monitor configurations, which enable you to send SQL traffic directly from the protected database. The database using the remote or local monitor connects directly to a Database Firewall.

Figure 1–1 Architecture of Oracle Database Firewall After Installation



General Oracle Database Firewall Installation Procedure

You will follow these general steps to install Oracle Database Firewall:

1. Plan the network scenario that best suits the needs of your site.

   See "Planning the Oracle Database Firewall Installation" on page 1-4 and "Deployment Scenarios" on page 1-4.

2. Ensure that your system meets the requirements described in this guide.

   See Chapter 2, "Oracle Database Firewall Preinstallation Requirements."

3. Install Oracle Database Firewall and Oracle Database Firewall Management Server.

   As part of this process, you will change the administrator password.

   See "Installing Database Firewall and Database Firewall Management Server" on page 3-2

4. Install the Analyzer.

   See "Installing the Analyzer" on page 3-8.

After you complete the installation, the Database Firewall administrator is responsible for configuring Oracle Database Firewall to monitor SQL data coming from your protected databases. See *Oracle Database Firewall Administration Guide*.

For a resilient pair (that is, high availability) configuration, you must periodically update Oracle Database Firewall. Chapter 4, "Updating the Oracle Database Firewall Software," provides instructions.

Planning the Oracle Database Firewall Installation

It is essential that Oracle Database Firewall monitors *all* traffic to the protected database. In general, this means that each Database Firewall must connect to a point in the network that is close to the database. An additional advantage of this approach is that Oracle Database Firewall will monitor less non-database traffic.

An alternative approach is to place an Oracle Database Firewall behind a client application, or at strategic points in the network. However, in all cases, you must ensure that database traffic does not bypass the Oracle Database Firewall system.

If statement blocking is not used, then you should use a spanning port to direct traffic to an Oracle Database Firewall port. The spanning port enables statement scanning without affecting network performance. The Oracle Database Firewall components connect using standard gigabit Ethernet network adapters.

If statement blocking is required, then you must place the Oracle Database Firewall in between the monitored database and the database clients and applications. In the unlikely event that an Oracle Database Firewall should fail, all traffic passes through, ensuring service continuity.

If users or processes have direct access to the database server system, consider using the Oracle Database Firewall local monitoring software to monitor traffic that originates from the database server itself.

Note: To simplify deployment, Oracle Database Firewall requires no change to the IP address of the database server or other network devices.

See Also: *Oracle Database Firewall Administration Guide* for detailed information about configuration, such as configuring local monitoring.

Deployment Scenarios

You can use any of the following deployment scenarios:

- **Install Database Firewall and Database Firewall Management Server onto one server.** In this scenario, the simplest, you install the Database Firewall onto one server, which uses an Oracle Linux environment. Then, you will install the Analyzer onto a client Microsoft Windows computer.
- **Install one or more Database Firewalls each onto a separate server and one Database Firewall Management Servers onto one server.** In this scenario, you install Database Firewall onto separate servers. Each of these servers communicates with one central Database Firewall Management Server. In turn, each protected database connects to a Database Firewall. You can install as many Database Firewalls as your site needs.
- **Configure one or more Database Firewalls and Database Firewall Management Servers for high availability.** In this scenario, you can build on the previous scenario by adding servers for high availability. For example, you can configure one additional Database Firewall Management Server for the first Management

Server, and you can configure an additional Database Firewall for each existing Database Firewall. One is used as the primary device, and the other is designated as the secondary device. The primary server performs all normal operations, while the secondary server monitors traffic. The secondary server alerts only when the primary server fails.

You can install a maximum of two Management Servers for your system, with one being used for high availability.

- **Configure a local monitor.** If you want to monitor the SQL data from connections made directly to the database server that do not pass through the network, then you can install the local monitoring software onto the protected database. (Be aware that local monitoring does not block SQL statements.) Then, configure this database to communicate directly with a Database Firewall, which in turn sends this SQL data to a Management Server. For detailed information about local monitoring, see *Oracle Database Firewall Administration Guide*.
- **Configure a remote monitor.** If you have many small databases in a distributed environment and you want Oracle Database Firewall to manage all of these small databases centrally, then you can install a remote monitor on a Linux server that can see all the database traffic that is sent to that Database Firewall. (Be aware that remote monitoring does not block SQL statements.) Typically, Database Firewall server is located close to the database and connected to a span port on a switch. The remote monitor runs from the database host's operating system and sends the database SQL traffic over the network to a Database Firewall that manages the remote monitor installations. For detailed information about remote monitoring, see *Oracle Database Firewall Administration Guide*.

For all of these scenarios, follow these guidelines:

- Install Oracle Database Firewall on a dedicated Intel x86 server. The Database Firewall installation formats the hard drives and any existing data on them is lost.
- Install Oracle Database Firewall in a physically secure, controlled environment.
- Ensure that the database network is logically or physically separate from the network that runs the Database Firewall applications. Configure the network firewalls, switches, taps, and hubs specifically to exclude traffic to and from unnecessary IP addresses.
- Ensure that the Database Firewalls are as close as possible, through the networking route, to the database server that you want to protect. The Management Server can be in any location, as long as it can access the other Database Firewall components.

> **Note:** In Database Policy Enforcement (DPE), or blocking, mode the IP address of the bridge must be on the same subnet as all protected databases deployed in DPE mode on that bridge. This restriction does not apply when using Database Activity Monitoring (DAM) mode.

- Ensure that Database Firewall has three network ports. The Management Server only needs one network port.
- Be aware that in DPE mode, the Database Firewall system blocks all IPv6 traffic, regardless of the policies set in place. In monitoring mode, the Database Firewall does not detect IPv6 traffic.

2

Oracle Database Firewall Preinstallation Requirements

This chapter contains:

Privileges Required to Perform the Installation

Any trusted user can install Oracle Database Firewall. You do not need administrative privileges to complete the installation.

Database Firewall and Management Server Hardware Requirements

You must install each Database Firewall and Management Server onto an Intel x86 server, which will be used solely for Oracle Database Firewall. The requirements for each are the same. Remember that the installation process re-images the computer, so do not use a computer that is used for other activities.

This section contains:

Checking the Oracle Linux Version

You must have Oracle Linux version 5.5 x86 DVD for the installation procedure. You can download Oracle Linux from the following Web site:

`https://edelivery.oracle.com/linux`

Checking the Memory Requirements

Each Intel x86 server must have at minimum 1 GB of RAM. You can check the memory by running the following command:

```
grep MemTotal /proc/meminfo
```

Checking the Disk Space

Each Intel x86 server must have a single hard drive with a minimum 80 GB of disk space. You can check the disk space by running the following command:

```
df -h
```

Checking the Network Interface Cards

You must have a minimum of three ports for each Intel x86 server that you will use for Database Firewall and Management Server. One network interface card (NIC) with three ports is sufficient.

Analyzer Hardware Requirements

You can install the Analyzer on Windows Vista or Windows XP.

Supported Database Versions

These databases (also called the protected databases) are the databases that you will monitor using Oracle Database Firewall. Table 2–1 shows the database products supported for regular monitoring, as well as Direct Database Interrogation (DDI), User Role Auditing (URA), Stored Procedure Auditing (SPA), and Local Monitor.

Table 2–1 Supported Databases with Supported Database Firewall Features

Supported Database	Direct Database Interrogation	User Role Auditing	Stored Procedure Auditing	Local Monitor
Oracle Database 8*i*				
Oracle Database 9*i*		Yes	Yes	Yes
Oracle Database 10*g*		Yes	Yes	Yes
Oracle Database 11g		Yes	Yes	Yes
Microsoft SQL Server 2000		Yes	Yes	
Microsoft SQL Server 2005	Yes	Yes	Yes	Yes
Microsoft SQL Server 2008	Yes	Yes	Yes	Yes
Sybase Adaptive Server Enterprise (ASE) versions 12.5.4 to 15.0.*x*		Yes	Yes	Yes
Sybase SQL Anywhere version 10.0.1	Yes	Yes	Yes	
IBM DB2 version 9.x (Linux, UNIX, Microsoft Windows)		Yes	Yes	

Requirements for Using the Remote Monitor

If you want to use the remote monitor software, ensure that the servers that you plan to use meet the following requirements:

- You can use the remote monitor on the Linux, UNIX, AIX platforms.
- The same database platforms that Oracle Database Firewall supports, as described in "Supported Database Versions" on page 2-2
- The following utilities:
  - GNU Netcat networking utility, which you can download from the following Web site:

    `http://netcat.sourceforge.net/`
  - Tcpdump packet analyzer; see the following Web site for more information:

    `http://www.tcpdump.org/`

Supported Language and Character Sets

Oracle Database Firewall and Database Firewall Analyzer are available in English only, but can support Unicode character sets.

Compatible Third-Party Products

You can use Oracle Database Firewall with the following third-party products:

- HP ArcSight Security Information Event Management (SIEM), which logs, analyzes, and manages network user activity that is recorded in syslog messages from different sources
- F5 BIG-IP ASM (Application Security Manager) (versions 9.5.*x* and 10.*x*), which provides protection against Web-based attacks

3

Installing Oracle Database Firewall

This chapter contains:

About the Installation Process

You will follow these general steps to install Oracle Database Firewall:

1. Install Oracle Database Firewall on an Intel x86 server that you plan to use exclusively for Database Firewall. Be aware that this installation process re-images this server, automatically installing the Oracle Linux operating system.

   The Database Firewall installation process also creates an Oracle Database Management Server on that server. If you only need to have one Database Firewall and Management Server installed on the same server, then you are ready to install the Analyzer.

2. If you want to install the Management Server onto a separate computer, then rerun the installer onto a second server using the Oracle Database Firewall Management Server 5.0 as the first disc. This server must be exclusively used for the Management Server.

   As with the Database Firewall, the installation process re-images this Intel x86 server to use Oracle Linux.

   After you run the installer for the Management Server on a separate Intel x86 server, then the Management Server on the first Database Firewall server is disabled because it is no longer needed.

3. If needed, install additional Database Firewalls onto their own individual Intel x86 servers, and then configure each to connect to a central Management Server.

4. For both the Database Firewall and Management Server installations, you must change the password for the `admin` user account the first time that you log in.

5. After you have installed the Database Firewalls and Management Servers, you can install the Analyzer onto a Windows computer.

Installing Database Firewall and Database Firewall Management Server

This section contains:

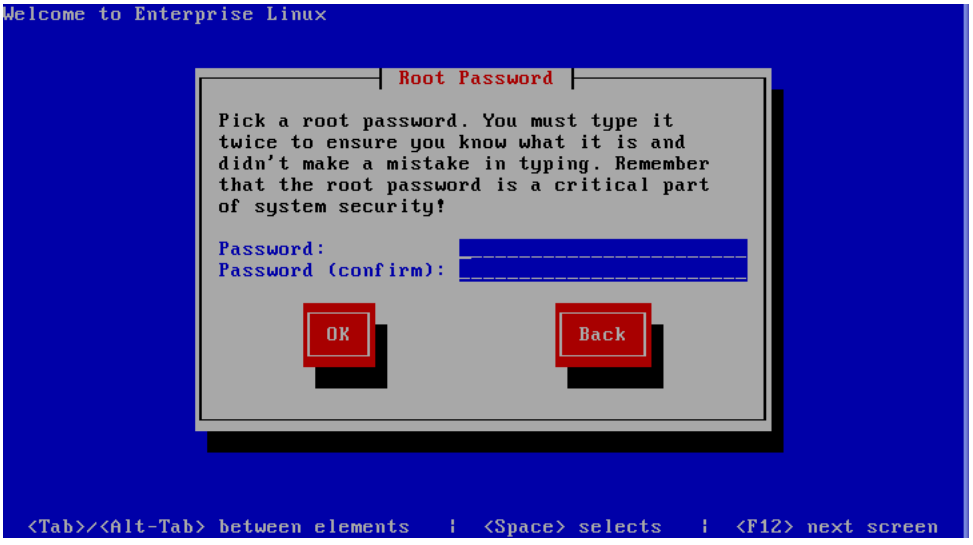
Step 1: Run the Oracle Database Firewall Installation Software

To install Database Firewall and Database Firewall Management Server:

1. In the Intel x86 system, insert the first disc of the component that you want to install:
   - **Database Firewall:** Insert the disc entitled `Oracle Database Firewall 5.0 - Disc 1`. Insert this disc to install the Oracle Database Firewall on a dedicated server, or to install both the Oracle Database Firewall and Oracle Database Firewall Management Server on the same server.
   - **Management Server:** Insert the disc entitled `Oracle Database Firewall Management Server 5.0`. Insert this disc to install the Oracle Database Firewall Management Server onto a separate server from the Oracle Database Firewall.
2. With the disc in the disc drive, restart the computer so it restarts from the CD/DVD ROM drive.

   Be aware that to start the installation process requires restarting the computer from the appropriate disc.
3. When prompted, insert the Oracle Linux DVD.
4. Press **Tab** to select the **OK** button, and then press **Return**.

   The Root Password screen appears.



5. In the **Password** field, create a root password, and then press the **Tab** key to move to the **Password (confirm)** field. Enter the password again, and then press **Enter**.

   Use the `root` account when you are requested to do so by Oracle Support. Create a password that is secure. Ways to create secure passwords are as follows:
   - Make the password between 8 and 30 characters and numbers.

- Include in the password at least one digit, one upper-case character, and one lower-case character.
- Do not use an actual word for the entire password.
- Combine two weaker passwords, such as `welcome` and `binky1` into `WelBinky1Come`.

The installer displays messages indicating that it is formatting and that the installation process is beginning.

6. When you are prompted for disc 2, remove the disc 1 (or `Oracle Database Firewall Management Server 5.0` if you had inserted it in Step 1) and then insert disc 2. Press **Enter**.
7. When you are prompted, remove disc 2 and then insert disc 3.
8. When you are prompted, remove disc 3 and then insert disc 1 (or `Oracle Database Firewall Management Server 5.0` if you had inserted it in Step 1).
9. When you are prompted, create a password for user `support`, and then press **Enter**.

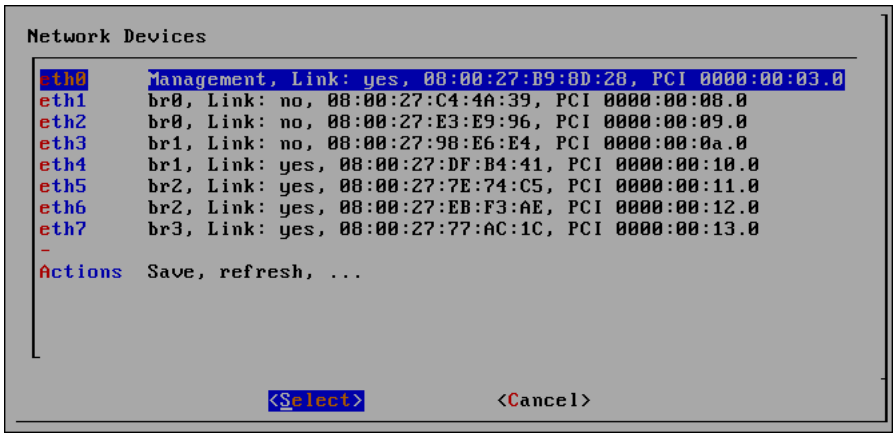
   Use the `support` account when you are requested to do so by Oracle Support. As you enter the password, be aware that no text, such as asterisks used to indicate the password that you are entering, appears.

   To create a password that is secure, see the guidelines listed in Step 5.

   In a moment, a message saying `Successfully configured system user "support"` appears. Press **Enter** to continue.
10. When you are prompted, confirm the password that you just created for user `support`, and then press **Enter**.
11. When prompted, create a password for the `sys` user.

    In a moment, a message saying `Successfully configured system user "sys"` appears. Press **Enter** to continue.

    The Network Devices screen appears, similar to the following:

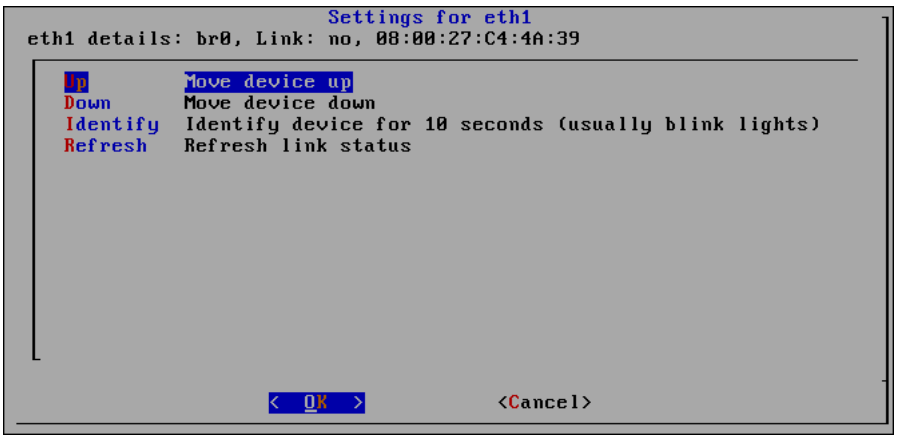


12. If you do not want to change the network device settings, then press the down arrow until you reach the bottom of the page. Select **Save**, and then go to Step 14.

    If you want to modify a network device connection, then in the Network Devices screen, select the network device connection that you want to use for Oracle Database Firewall or Management Server.

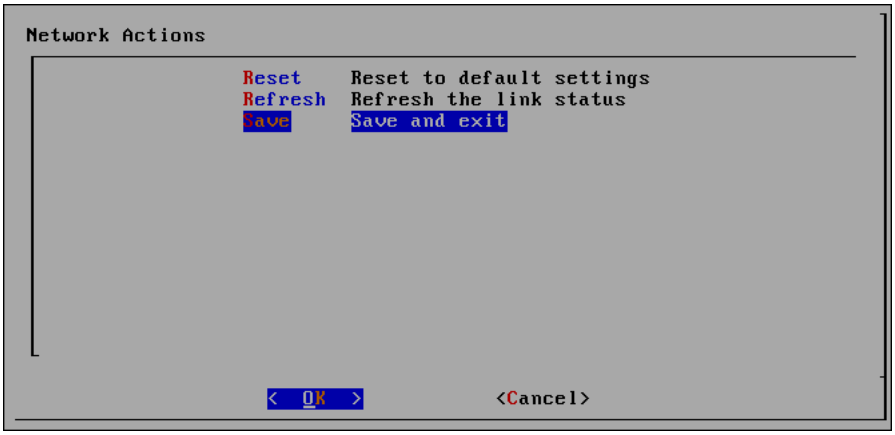
Press the **Tab** key to move through the list. To make the section, press **Enter**. The Settings screen appears next.

For example:



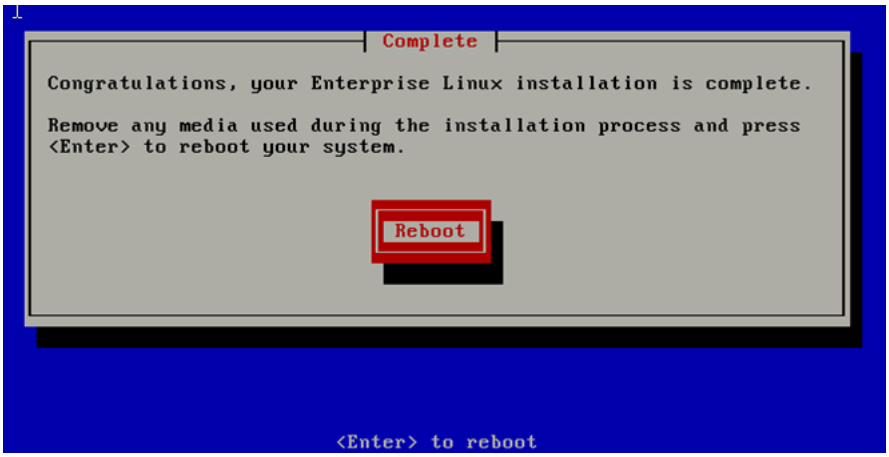
13. To change the settings from Step 12, in the Settings screen, select from the following choices. These settings enable you to map the physical ports to the Management Server interfaces and bridges.
    - **Up:** Moves the device up in the list.
    - **Down:** Moves the device down in the list.
    - **Identify:** Identifies the device for 10 seconds, usually with blinking lights.
    - **Refresh:** Refreshes the list of links on the previous page.
14. When you complete the settings, click **OK**.

    The Network Actions screen appears next.

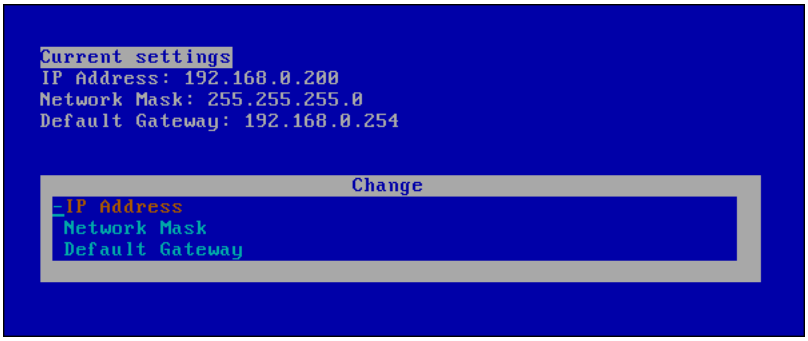


15. In the Network Actions screen, select **Save** and then press **Enter**.

    In a moment, a message saying `Saved network settings successfully` appears. Press **Enter**.
16. When the Complete screen appears, remove any media that you used during the installation process and then press **Enter** to restart your system. (This configuration step may take a while because an Oracle database is silently installed.)



17. After the Database Firewall has rebooted successfully, you will be placed back at this screen.



The Database Firewall has completed installation. There are seven other terminal screens that can be accessed by pressing Alt-F2 through Alt-F8. From these screens you can log in as root and/or support to view logs on the Database Firewall. You should not access any files directly on Database Firewall unless directed by Oracle Support. The Alt-F9 terminal can be used to view any startup messages.

When you see this screen, continue to the next step to configure network settings.

18. Select an option (**IP Address**, **Network Mask**, or **Default Gateway**) by pressing the **Up** arrow or the **Down** arrow, followed by **Enter**.

    The dash sign (**-**) shows the currently selected option. Press **Esc** if you want to return to the previous screen.

19. Select the required value in each field by pressing the **Up** arrow or the **Down** arrow, followed by **Enter**.

    Note the following:

    - **IP Address** is the address that you will use in the URL for the Database Firewall Administration Console. Make a note of this IP address for any user who wants to use the Administration Console.
    - In most cases, you do not need to change the **Network Mask** settings.
    - Set **Default Gateway** to `0.0.0.0` if you are not using a gateway.

20. When prompted, select **Accept** to accept the setting or click **Back** to return to the previous screen and reenter the IP address.

This step completes the configuration process, and your computer is ready to use. You do not need to perform any additional steps, such as restarting your computer.

Step 2: Start the Administration Console and Change the admin Password

The installation process creates an Administration Console on each Database Firewall and Management Server server. After you complete the installation, you should log in to the console and change the password for the default administrative user, `admin`.

The first time that you start the Administration Console for either a Database Firewall or for a Management Server, you will be prompted to change the default password.

1. Start a Web browser.
2. Enter the following URL:

   `https://`*`ip_address`*`/user/login`

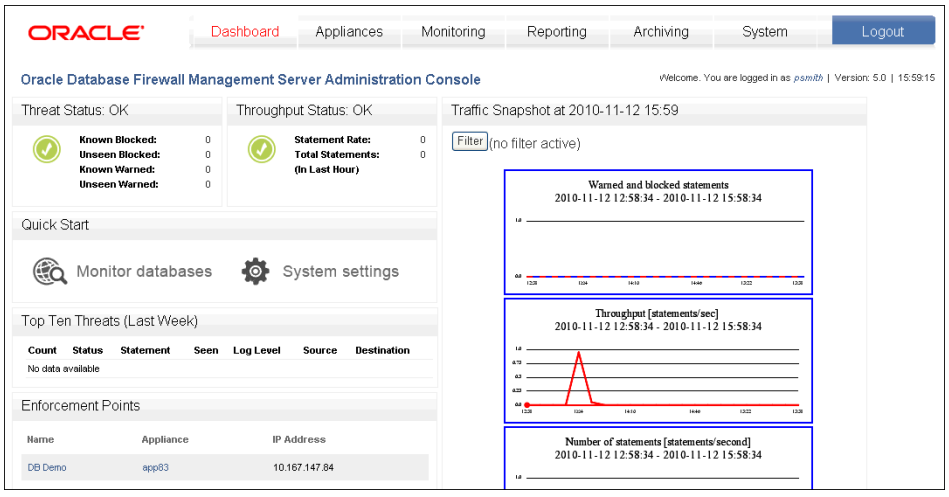
   In this specification:

   - *`ip_address`*: Enter the IP address setting that you created in Step 19 under "Step 1: Run the Oracle Database Firewall Installation Software" on page 3-2.
3. In the Web browser, add this URL to your Favorites to make it easy to access.
4. In the Login page, enter the following credentials:

   - **Login ID:** `admin`
   - **Password:** `admin`

   When prompted, enter a new password. Create a password that is secure. See the guidelines that are listed in Step 5 under "Step 1: Run the Oracle Database Firewall Installation Software" on page 3-2.

   The Administration Console appears. The following window shows how the Administration Console typically appears for a Management Server system.



Ports That Oracle Database Firewall Uses

This section lists ports that Oracle Database Firewall uses.

Table Table 3–1 shows ports for services provided by the Database Firewall or Management Server used by outside users of the system. Access to all these services can be controlled within the Database Firewall system. If external network firewalls

are used, these ports must be open to allow connections from the users (clients) of these services to the Database Firewall system(s).

Table 3–1 Ports for Services Provided by Database Firewall or Management Server

Port	Protocol Family	Protocol	Purpose	Notes
22	TCP	SSH	Command line access to system	
161	UDP	SNMP	SNMP access	
443	TCP	HTTPS	Administration Console (web interface)	This port can be changed in the administration console
1521	TCP	Oracle Database	Secure log access for external reporting	
4560	TCP	DBFW internal protocol	Analyzer access to traffic log	
1514	TCP	TCP syslog over SSL	Incoming syslog messages from external web application firewall	
4600 - 4680	TCP	DBFW internal protocol	Incoming traffic captures from Remote Monitor	When setting up these Enforcement Points in the Administration Console, use the port numbers indicated in the Enforcement Point setup page.
5514 - 5593	TCP	Syslog	Incoming WAF (F5) violation alerts	When setting up these Enforcement Points in the Administration Console, use the port numbers indicated in the Enforcement Point setup page.

Table Table 3–2 shows ports for external services that may be used by the Database Firewall. If external network firewalls are used, the relevant ports must be open so that the Database Firewall can use these services as a client.

Table 3–2 Ports for External Network Access by Database Firewall or Management Server

Port	Protocol Family	Protocol	Purpose	Notes
25	TCP	SMTP	Email delivery	
123	UDP and TCP	NTP	Time synchronization	
514	UDP, or configured as TCP	Syslog	Syslog alerts	For TCP-transport connections to syslog server(s) the port must be configured in the Administration Console
514	UDP, or configured as TCP	Proprietary ArcSight protocol over syslog transport	DBFW alerts	For TCP-transport connections to ArcSight server(s) the port must be configured in the Administration Console.
514	TCP	Syslog	WAF (F5) alerts	The port can be changed from the Administration Console.

Table Table 3–3 shows ports for services that are used between the Database Firewall and any Database Firewall Management Server. If an external network firewall is placed between these systems, then the relevant ports must be opened.

Table 3–3 Ports for Database Firewall Internal TCP Communication

Port	Protocol Family	Protocol	Direction	Purpose
443	TCP	HTTPS	Database Firewall accepts connections from Management Server	Command interface
1514	TCP	SSL	Management Server accepts connections from Database Firewall	Event reporting and monitoring

Installing the Analyzer

After you have installed the Database Firewall and Management Server, you are ready to install the Analyzer.

To install Oracle Database Firewall Analyzer:

1. Insert disc entitled `Oracle Database Firewall Utilities 5.0` into your Windows disc drive and then locate the `OracleDatabaseFirewallAnalyzerInstaller.exe` file.

   This executable is located at the root level of the disc.

2. Double-click the `OracleDatabaseFirewallAnalyzerInstaller.exe` file to install the Oracle Database Firewall Analyzer.

   The Welcome to the Oracle Database Firewall Analyzer Setup Wizard page appears.

3. Click **Next**.

   The Choose Install Location page appears. By default, the destination folder is within the Oracle folder in the Program Files folder.

4. Click **Browse** if you want to install the Oracle Database Firewall Analyzer Installer in a different location. Click **Next**.

   The Choose Start Menu Folder page appears.

5. Click **Install**.

   The Completing the Oracle Database Firewall Analyzer Setup Wizard page appears.

6. Click **Finish**.

   The Oracle Database Firewall Analyzer is installed.

Increasing the Oracle Database Firewall Default Disk Space

The Oracle Database Firewall (standalone or managed) will expand to use 100 GB of disk space. The Management Server will expand to use 500 GB of disk space. To use more space for either server requires manual changes. This section explains how to extend their partition sizes. Ideally, you should perform these steps after the Database Firewall installation and before you configure any enforcement points.

To increase the standalone Database Firewall and the Management Server disk space:

1. If your Database Firewall system is already in use (for example, you have configured enforcement points), then archive the configuration, traffic log files and audit files.

2. Log in to the computer as user `root`.
3. Run the `vgs` command to find the amount of free disk space.

   For example:

   ```
   vgs

   VG       #PV   #LV   #SN Attr     VSize     VFree
   new_vg     3     1     1 wz--n-   120.03G   238.25G
   ```

   Next, decide how you want to allocate space for the Oracle partition and the log file partition.

   - **Managed Database Firewall:** Add 100 percent for the extra space. For example, if the managed Database Firewall uses 100 GB of disk space, you should add 100 GB of space.
   - **Standalone Database Firewall or a Management Server:** For a standalone Database Firewall or a Management Server, Oracle recommends that you allocate a third of the extra space to the Oracle partition, and two thirds of the space to the log file partition. You should leave some extra space in case you want to change the partition layout in the future.

     The following examples allocate 66 GB for the Oracle partition and 132 GB for the log file partition, leaving 40.25 GB free.
4. For the Oracle partition, run the following command to change the size of the logical volume group for the `/var/lib/oracle` directory.

   ```
   lvextend -L+space_amountG /dev/vg_root/lv_oracle
   ```

   This directory is where the Oracle database resides. Replace *`space_amount`* with a value for the amount of space that you want to add. For example:

   ```
   lvextend -L+66G /dev/vg_root/lv_oracle
   ```
5. For the log file partition, run the following command to extend the partition where the compressed log files are stored.

   ```
   lvextend -L+space_amountG /dev/vg_root/lv_var_dbfw
   ```

   Replace *`space_amount`* with a value for the amount of space that you want to add. For example:

   ```
   lvextend -L+132G /dev/vg_root/lv_var_dbfw
   ```
6. Run the following commands to ensure that each partition uses all the space that is now available to it.

   ```
   resize2fs /dev/vg_root/lv_oracle

   resize2fs /dev/vg_root/lv_var_dbfw
   ```
7. Increase the size of the `USERS` tablespace by following the instructions in article 1332492.1 on the Oracle support site: `https://support.oracle.com`.

What's Next?

At this stage, Oracle Database Firewall, Management Server, and the Analyzer are installed in your system. The next step is for the Database Firewall administrator to configure the following connections:

- **The connections between each Database Firewall and the Management Server.** Oracle strongly recommends that you perform this step right after you complete the installation. Chapter 2 and Chapter 3 in *Oracle Database Firewall Administration Guide* cover this topic.
- **The connections required for a high availability environment.** Chapter 4 in *Oracle Database Firewall Administration Guide* covers this topic.
- **User accounts for your site.** See *Oracle Database Firewall Administration Guide* for detailed information about configuring users.
- **The ability of the Database Firewall to track stored procedure and user account information in the protected database.** Chapter 5 and Chapter 6 in *Oracle Database Firewall Administration Guide* cover this topic.
- **The connections between each Database Firewall and the protected database that it monitors.** Chapters 7 through 10 in *Oracle Database Firewall Administration Guide* cover this topic.

After this configuration is complete, users who are responsible for using the Analyzer can begin to create policies and monitor SQL traffic, as described in *Oracle Database Firewall Security Management Guide*.

4

Updating the Oracle Database Firewall Software

This chapter contains:

About Updating the Oracle Database Firewall Software

This chapter explains how to update the Oracle Database Firewall software in Management Servers or Database Firewalls. The procedures described here apply to both stand-alone Database Firewalls and to Database Firewalls that are in a resilient pair for a high availability configuration.

If the installation contains paired Oracle Database Firewall Management Servers and Oracle Database Firewalls, then you must upgrade the Oracle Database Firewall Management Servers first.

For detailed information about how Oracle Database Firewall works in a high availability environment, see *Oracle Database Firewall Administration Guide*.

Procedure for Updating an Oracle Database Firewall

Caution: You must follow the specific procedures detailed in the README file of every Oracle Database Firewall update. The procedure given here has general instructions only.

To update Oracle Database Firewall or Management Server:

Note: If you use a Management Server and managed Database Firewalls, then perform this procedure on the Management Server first, then on the Database Firewalls.

1. Copy the provided RPM file onto the server of the Database Firewall or the Management Server by running a command similar to the following:

   ```
   scp update_RPM_file support@DBFW_or_MS_ip_address:/tmp/
   ```

2. Log in to the Database Firewall or Management Server as user `root`.

3. Run these two commands:

```
/bin/rpm --freshen --repackage update_RPM_file

/bin/ls /var/spool/repackage -t | /usr/bin/head -n1 >
/usr/local/dbfw/updates/lastrpm
```

4. Reboot the server.
5. To update to the new Analyzer version, run the installer on the machine where you have the Analyzer installed.

5

Removing Oracle Database Firewall

This chapter contains:

Removing Database Firewall and Management Server

You cannot deinstall the Database Firewall and Management Server. However, you can reimage the computers on which you have installed these components.

Removing Oracle Database Firewall Software Settings

This section contains:

Removing Oracle Database Firewall from Oracle Databases

To disable local monitoring and remove the Oracle Database Firewall-associated user accounts and other objects from Oracle databases:

1. From the Management Server, log in to the Administration Console as the `admin` user.
2. Disable local monitoring as follows:
   a. Click the **Monitoring** tab.
   b. Click the **Settings** button for the appropriate enforcement point.
   c. Deselect the **Activate Database Interrogation**, **Activate Local Monitor**, **Activate Stored Procedure Monitoring**, and **Activate Stored Procedure Auditing** check boxes.
   d. Click **Save**.

3. From the `Oracle Database Firewall Utilities 5.0` disk, copy the following scripts to the server on which Oracle Database is installed:
   - **dcam_drop.sql and dcam_remove_user.sql:** Disables local monitoring. Located in the `database/localmonitor` directory in compressed format (`.tar` and `.zip` files named for the database product).
   - **spa_drop.sql:** Disables stored procedure auditing. Located in the `database/spa` directory in compressed format (`.tar` and `.zip` files named for the database product).
   - **ura_drop.sql:** Disables user role auditing. Located in the `database/ura` directory in compressed format (`.tar` and `.zip` files named for the database product).
4. Review each script to ensure that the user in the script has the appropriate privileges to perform the tasks.

   For example, if the database has been enabled with Oracle Database Vault, you must edit the scripts so that a user who has been granted the `DV_ACCTMGR` role can drop the user accounts.

   You can find this user by running the following query in SQL*Plus:

   ```
   SQL> SELECT USERNAME FROM USER_ROLE_PRIVS WHERE GRANTED ROLE = 'DV_ACCTMGR';
   ```

   Enter the granted role, `DV_ACCTMGR`, in upper-case letters, because that is the case in which Oracle Database stores user names and roles.
5. Log in to Oracle Database as user `DBFW_CONSOLE_ACCESS`.

   For example:

   ```
   sqlplus dbfw_console_access
   Enter password: password
   Connected.
   SQL>
   ```
6. Run the `dcam_drop.sql` script.

   ```
   SQL> @dcam_drop.sql
   ```
7. Connect as a user who has privileges to drop users.

   For example, if the database was enabled with Oracle Database Vault, then log in as the `DV_ACCTMGR` user. If not, then log in as a user with the `SYSDBA` privilege.

   For example:

   ```
   connect sys/as sysdba
   Enter password: password
   Connected.
   SQL>
   ```
8. Run each script as follows:

   ```
   SQL> @ddi_drop_user.sql
   SQL> @dcam_remove_user.sql
   SQL> @spa_drop.sql
   SQL> @ura_drop.sql
   ```
9. Exit SQL*Plus.

   ```
   SQL> exit
   ```

10. If necessary, delete the `localmonitoring` directory.

Removing Oracle Database Firewall from Microsoft SQL Server Databases

To disable local monitoring and remove the Oracle Database Firewall-associated user accounts and other objects from SQL Server databases:

1. From the Management Server, log in to the Administration Console as the `admin` user.
2. Disable local monitoring as follows:
   a. Click the **Monitoring** tab.
   b. Click the **Settings** button for the appropriate enforcement point.
   c. Deselect the **Activate Database Interrogation**, **Activate Local Monitor**, **Activate Stored Procedure Monitoring**, and **Activate Stored Procedure Auditing** check boxes.
   d. Click **Save**.
3. From the `Oracle Database Firewall Utilities 5.0` disk, copy the following scripts to the server on which Microsoft SQL Server is installed:
   - **ddi_drop_user.sql:** Disables direct database interrogation (DDI). Located in the `database/ddi` directory in compressed format (`.tar` and `.zip` files named for the database product).
   - **dcam_drop.sql and dcam_remove_user.sql:** Disables local monitoring. Located in the `database/localmonitor` directory in compressed format (`.tar` and `.zip` files named for the database product).
   - **spa_drop.sql:** Disables stored procedure auditing. Located in the `database/spa` directory in compressed format (`.tar` and `.zip` files named for the database product).
   - **ura_drop.sql:** Disables user role auditing. Located in the `database/ura` directory in compressed format (`.tar` and `.zip` files named for the database product).
4. Review each script to ensure that the user in the script has the appropriate privileges to perform the tasks.
5. If you want to remove the local monitoring objects, then log in to the Microsoft SQL Server database as user `DBFW_CONSOLE_ACCESS` and run the `dcam_drop.sql` script.

   ```
   sqlcmd -S server_name -U dbfw_console_access -P password
   1> :r dcam_drop.sql
   ```

6. Log in to the Microsoft SQL Server database as a user who has privileges to drop user accounts.

   For example:

   ```
   sqlcmd -S server_name -U sa -P password
   ```

7. Run each script as follows:

   ```
   1> :r ddi_drop_user.sql
   2> :r dcam_remove_user.sql
   3> :r spa_drop.sql
   4> :r ura_drop.sql
   ```

8. Exit the Microsoft SQL Server database.

Removing Oracle Database Firewall from Sybase ASE and SQL Anywhere Databases

To disable local monitoring and remove Oracle Database Firewall user accounts and other objects from Sybase ASE and SQL Anywhere databases:

1. From the Management Server, log in to the Administration Console as the `admin` user.
2. Disable local monitoring as follows:
   a. Click the **Monitoring** tab.
   b. Click the **Settings** button for the appropriate enforcement point.
   c. Deselect the **Activate Database Interrogation**, **Activate Local Monitor**, **Activate Stored Procedure Monitoring**, and **Activate Stored Procedure Auditing** check boxes.
   d. Click **Save**.
3. From the `Oracle Database Firewall Utilities 5.0` disk, copy the following scripts to the server on which Sybase ASE is installed:
   - **ddi_drop_user.sql:** Disables direct database interrogation (DDI) from Sybase SQL Anywhere databases. Located in the `database/ddi` directory in compressed format (`.tar` and `.zip` files named for the database product).
   - **dcam_drop.sql and dcam_remove_user.sql:** Disables local monitoring. Located in the `database/localmonitor` directory in compressed format (`.tar` and `.zip` files named for the database product).
   - **spa_drop.sql:** Disables stored procedure auditing. Located in the `database/spa` directory in compressed format (`.tar` and `.zip` files named for the database product).
   - **ura_drop.sql:** Disables user role auditing. Located in the `database/ura` directory in compressed format (`.tar` and `.zip` files named for the database product).
4. Review each script to ensure that the user in the script has the appropriate privileges to perform the tasks.
5. If you want to remove the local monitoring objects, then log in to the Sybase ASE database as user `DBFW_CONSOLE_ACCESS` and run the `dcam_drop.sql` script.

   ```
   sqlcmd -S server_name -U dbfw_console_access -P password
   1> :r dcam_drop.sql
   ```

6. Log in to the Sybase ASE database as a user who has privileges to drop user accounts.

   For example:

   ```
   sqlcmd -S server_name -U sa -P password
   ```

7. Run each script as follows:

   ```
   1> :r dcam_remove_user.sql
   2> :r spa_drop.sql
   3> :r ura_drop.sql
   ```

8. If you ran the `dcam_drop.sql` script, then restart the Sybase ASE database.

9. Exit the Sybase ASE database.
10. Log in to the Sybase SQL Anywhere database as a user who has privileges to drop user accounts.

    For example:

    ```
    sqlcmd -S server_name -U sa -P password
    ```

11. Run the `ddi_drop_user.sql` script as follows:

    ```
    1> :r ddi_drop_user.sql
    ```

Removing Oracle Database Firewall from IBM DB2 SQL Databases

To remove Oracle Database Firewall stored procedure and user role auditing privileges from user accounts on IBM DB2 SQL databases:

1. Log in to the IBM DB2 Windows, UNIX, or Linux database that you used to audit stored procedures or user roles.
2. Revoke the following privilege from the user account that is responsible for stored procedure auditing:

    ```
    revoke select on syscat.routines from user
    ```

3. Revoke the following privileges from the user account that is responsible for user role auditing:

    ```
    revoke select on sysibmadm.authorizationids from user
    revoke select on syscat.dbauth from user
    ```

Removing the Remote Monitor Software

To remove the remote monitor software:

1. As user `root`, log in to the Linux server where you installed the remote monitor files, the `remote-agent` script and the `remote-agent.conf` file.
2. Go to the directories where you copied these files.

    The `remote-agent` script should be in the `/bin` directory and the `remote-agent.conf` file should be in the `/etc` directory.
3. For the `remote-agent` script, stop its process.
4. Delete the `remote-agent` script and the `remote-agent.conf` file.
5. If you updated your startup script to run the `remote-agent` script, then remove the reference to this script from the startup script.
6. As user `admin`, log in to the Administration Console for the Database Firewall that runs the remote monitor.
7. Select the **Monitoring** tab.

    By default, the Enforcement Points page appears. If it does not, then click **List** in the Enforcement Points menu on the left side of the page.
8. Find the enforcement point for the remote monitor, and then click the **Settings** button for that enforcement point.

    The Monitor Settings page appears.
9. Clear the **Activate Remote Monitor** check box.

10. Scroll to the end of the Monitor Settings page, and then click the **Save** button.

Removing Oracle Database Analyzer

To remove Oracle Database Analyzer:

1. From the Windows Control Panel, select **Add or Remove Programs**.
2. From the Currently installed programs list, select **Oracle Database Firewall Analyzer**.
3. Click the **Change/Remove** button.
4. In the Oracle Database Firewall Analyzer Uninstall window, click the **Uninstall** button.
5. When the Completing the Oracle Database Firewall Analyzer Unistall Wizard page appears, click **Finish**.

Index